IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please ADD new claim 48 and AMEND the claims in accordance with the following:

1. (currently amended) A system for managing information comprising:

a communication request monitor unit which monitors a communication request;

a management unit which selects a countermeasure based upon information notified from the communication request monitor unit;

a performing unit which performs a countermeasure in response to an instruction from the management unit,

wherein said management unit comprises:

a database which manages a notification content from the communication request monitor unit and the countermeasure that the performing unit performs such that the notification content and the countermeasure correspond to each other, and

a selection unit which selects the countermeasure from various angles based upon the database and mounting information, operation information, and/or security information to be performed;

an information collection unit which collects information related to a kind, a content, an order, and a time interval of two or more communications in a ~~proceeding~~ progress process of an attack event or a leakage event, such that the information is collected through an attack caused by induction, so that the collected information is analyzed to be recognized as an attack pattern to be used to predict a future attack which may occur; and

a reflection unit which reflects the information collected and regulated by the information collection unit upon the database, to thereby predict a possible attack event or a leakage event in advance, and to avoid the predicted attack event or leakage event before execution of the predicted attack event or leakage event, wherein the information notified by the communication request monitor unit and/or countermeasure selected by the management unit are weighted.

2. (cancelled)

3. (cancelled)

4. (previously presented) The system according to claim 1, wherein based upon which of the mounting information, the operation management information and/or the security information a countermeasure is selected can be setting-changed according to the selection of a user.

5. (original) The system according to claim 1, wherein the communication request monitor unit, management unit, and the performing unit are provided in plurality.

6. (original) The system according to claim 5, wherein the communication request monitor units, management units, and the performing units cooperate with each other between the same type or different types thereof to exchange information.

7. (cancelled)

8. (previously presented) The system according to claim 1, wherein a weight coefficient for the weighting can be arbitrarily set by a user.

9. (previously presented)The system according to claim 1, wherein a weight coefficient for the weighting is set based upon the mounting information, operation management information and/or security information.

10. (original) The system according to claim 1, wherein the database holds information notified by the communication request monitor unit in time series, and the selection unit selects a countermeasure based upon the time series information stored in the database.

11. (original) The system according to claim 5, further comprising a site map formation unit which forms a site map representing a spatial arrangement of a website based upon the information notified by the plural communication request monitor unit.

12. (previously presented) The system according to claim1, further comprising a site map formation unit which forms a site map representing a spatial arrangement of a website based upon the information notified by the plural communication request monitor unit.

13. (original) The system according to claim 10, further comprising a site map formation unit which forms a site map representing a spatial arrangement of a website based upon the information notified by the plural communication request monitor unit.

14. (previously presented) The system according to claim 5, further comprising a monitor condition notification unit which notifies the communication request monitor unit of the kind and/or time of a communication to be a monitor object based upon a site map formed by a site map formation unit.

15. (previously presented) The system according to claim 1, further comprising a monitor condition notification unit which notifies the communication request monitor unit of the kind and/or time of a communication to be a monitor object based upon a site map formed by a site map formation unit.

16. (original) The system according to claim 10, further comprising a monitor condition notification unit which notifies the communication request monitor unit of the kind and/or time of a communication to be a monitor object based upon the a site map formed by the site map formation unit.

17. (original) The system according to claim 1, wherein the management unit gives a request to a website existing in a network and automatically updates the database based upon information replied in response to the request.

18. (previously presented) The system according to claim 17, wherein the request is performed at a user's suggestion.

19. (original)The system according to claim 1, wherein the management unit automatically updates the database based upon information automatically transmitted from a website existing in a network.

20. (previously presented) The system according to claim 19, wherein the information automatically transmitted from a website existing in a network is taken in the database in response to a request of a user.

21. (currently amended) The system according to claim 1, further comprising:

a vulnerability present unit which provides vulnerability of the system; and

~~an~~ the information collection unit which collects information related to an attack the vulnerability presented by the vulnerability present unit.

22. (original) The system according to claim 1, further comprising an investigation unit investigating an outgoing source of a communication content and a determination unit which determines whether or not a website is made a stepping-stone by an ill-intentioned person based upon an investigation result by the investigation unit.

23. (original) The system according to claim 1, further comprising a decoy unit leading a communication to a location different from an attack object to avoid an attack.

24. (currently amended) A method of managing information comprising:

~~a communication request monitor step~~ monitoring a communication request by a communication request monitor unit;

~~a selection step in which a management unit selects~~selecting, via a management unit, a countermeasure from various angles based upon a database and mounting information, operation management information, and/or security information, wherein the database manages a notification content notified by the communication request monitor step and a countermeasure to be performed such that the notification content and the countermeasure correspond to each other; and

~~a performing step in which a performing unit performs~~ performing, via a performing unit, the countermeasure selected in response to an instruction from the management ~~step~~unit;

~~an information collection step~~ collecting information related to a kind, a content, an order, and a time interval of two or more communications in a ~~proceeding~~ progress process of an attack event or a leakage event, such that the information is collected through an attack caused by induction, so that the collected information is analyzed to be recognized as an attack pattern

to be used to predict a future attack which may occur; and

~~a reflection step~~ reflecting the information collected and regulated by the information collection step upon the database, to thereby predict a possible attack event or a leakage event in advance, and to avoid the predicted attack event or leakage event before execution of the predicted attack event or leakage event, wherein the information notified by the communication request monitor unit and/or countermeasure selected by the management unit are weighted.

25. (cancelled)

26. (cancelled)

27. (previously presented) The method according to claim 24, wherein based upon which of the mounting information, the operation management information and/or the security information a countermeasure is selected and can be setting-changed according to the selection of a user.

28. (original) The method according to claim 24, wherein the communication request monitor unit, management unit, and the performing unit are provided in plurality.

29. (original) The method according to claim 28, wherein the respective plurality of communication request monitor units, management units, and performing units cooperate with each other between the same type or different types thereof to exchange information.

30. (cancelled)

31. (original) The method according to claim 30, wherein a weight coefficient for the weighting can be arbitrarily set by a user.

32. (previously presented) The method according to claim 24, wherein a weight coefficient for the weighting is set based upon the mounting information, operation management information and/or security information.

33. (currently amended) The method according to claim 24, wherein the database holds information notified by the communication request monitor unit in time series, and ~~the~~

~~selection step selects~~ a countermeasure is selected based upon the time series information stored in the database.

34. (currently amended) The method according to claim 28, further comprising ~~a site map formation step~~ forming a site map representing a spatial arrangement of a website based upon the information notified by the communication request monitor units.

35. (currently amended) The method according to claim 24, further comprising ~~a site map formation step~~ forming a site map representing a spatial arrangement of a website based upon the information notified by the communication request monitor units.

36. (currently amended) The method according to claim 33, further comprising ~~a site map formation step~~ forming a site map representing a spatial arrangement of a website based upon the information notified by the communication request monitor units.

37. (currently amended) The method according to claim 28, further comprising ~~a monitor condition notification step~~ notifying the communication request monitor units of the kind and/or time of a communication to be a monitor object based upon ~~the~~ a site map formed ~~by the site map formation step~~.

38. (currently amended) The method according to claim 24, further comprising a ~~monitor condition notification step~~ notifying the communication request monitor units of the kind and/or time of a communication to be a monitor object based upon ~~the~~ a site map formed ~~by the site map formation step~~.

39. (currently amended) The method according to claim 33, further comprising a ~~monitor condition notification step~~ notifying the communication request monitor units of the kind and/or time of a communication to be a monitor object based upon ~~the~~ a site map formed ~~by the site map formation step~~.

40. (original) The method according to claim 24, wherein the management unit gives a request to a website existing in a network and automatically updates the database based upon information replied in response to the request.

41. (original) The method according to claim 40, wherein the request is performed in response to a request of a user.

42. (original) The method according to claim 24, wherein the management unit automatically updates the database based upon information automatically transmitted from a website existing in a network.

43. (original) The method according to claim 42, wherein the database is automatically update based on the information transmitted from a website existing in a network in response to a request of a user.

44. (currently amended) The method according to claim 24, further comprising ~~a vulnerability present step of~~ providing vulnerability of the system; and ~~an~~ the information collection step collecting information related to an attack against the vulnerability provided ~~in the vulnerability present step~~.

45. (currently amended) The method according to claim 24, further comprising ~~an investigation step~~ investigating an outgoing source of a communication content and ~~a determination step~~ determining whether ~~or not~~ a website is made a stepping-stone by an ill-intentioned person based upon an investigation result ~~by the investigation step~~.

46. (original) The method according to claim 24, further comprising a decoy unit leading a communication to a location different from an attack object to avoid an attack.

47. (currently amended) A computer readable medium comprising a method performed by a computer, the method comprising:

monitoring communication requests;

outputting a notification in case of an abnormality;

selecting a countermeasure from various angles based upon a database and mounting information, operation management information, and/or security information, wherein the database manages a content of the notification and a corresponding countermeasure;

performing a countermeasure against the abnormality based on the selected countermeasure;

collecting information related to a kind, a content, an order, and a time interval of two or

more communications in a proceeding process of an attack event or a leakage event, such that the information is collected through an attack caused by induction, so that the collected information is analyzed to be recognized as an attack pattern to be used to predict a future attack which may occur; and

reflecting the information collected and regulated by the information collected upon the database, to thereby predict a possible attack event or a leakage event in advance, and to avoid the predicted attack event or leakage event before execution of the predicted attack event or leakage event.

48. (new) A method of predicting attack of an omen in a network, the method comprising:

collecting and storing underground information, damage information and information related to an attack of an omen collected through the attack caused by induction, and analyzing the information collected and stored to be recognized as an attack pattern;

storing countermeasures corresponding to the stored attack pattern;

predicting and preventing a future attack by performing a countermeasure corresponding to the stored attack pattern.